Online safety policy

Inspiring a love for lifelong learning

Approved by:	FGB Autumn 2020
Next review due by:	Autumn 2024

Key Details

Designated Safeguarding Lead (s): Sarah Tarrant

Named Governor with lead responsibility: Paul Goulden

This policy will be reviewed regularly and revised following any concerns and/or updates to national and local guidance or procedures.

Contents

1. Policy Scope and Aims

- Ashford Park believes that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all pupils and staff are protected from potential harm online.

- Ashford Park identifies that the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life.

- Ashford Park believes that pupils should be empowered to build resilience and to develop strategies to manage and respond to risk online.

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors

- Deliver an effective and positive approach to online safety, which empowers us to protect and educate the whole school community in its use of technology

- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

2. Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education (2022), and its advice for schools on preventing and tackling bullying. It also refers to the Department's guidance on protecting children from radicalisation and Teaching online safety in school.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010.

The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring this policy.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by RM and Soft Egg.

The governor responsible for monitoring online safety will:

- Ensure that they have read and understand this policy

- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (Appendix 2)

3.2 The Head teacher

The Head teacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The Designated Safeguarding Lead

Online safety is the responsibility of the DSL and Curriculum lead. Responsibilities include:

- Ensuring that staff understand this policy and that it is being implemented consistently throughout the school

- Working with the School Business Manager (SBM), Soft Egg and RM, as necessary, to address any online safety issues or incidents

- Ensuring that any online safety incidents are logged (see Appendix 4) and dealt with appropriately in line with this policy

- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school Behaviour for Learning Policy through behaviour for learning online procedure

- Working with SBM, RM and Soft Egg to update and deliver staff training on online safety (Appendix 3 contains a self-audit for staff on online safety training needs)

- Keep up-to-date with current research, legislation and trends regarding online safety and communicate this with the school community, as appropriate.

- Work with staff to coordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day.

- Liaising with other agencies and/or external services if necessary

- Providing regular reports on online safety in school to the headteacher and/or governing board

3.4 The IT Leadership and Management (SBM, DSL, Curriculum Lead, RM, Soft Egg)

This team is responsible for monitoring:

- RM filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material (illegal content)

- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly

- Monitoring and working with RM and Soft Egg to ensure that ICT systems are regularly monitored

- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

- Ensuring that any online safety incidents are logged (see Appendix 4) and dealt with appropriately in line with this policy

- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy

- Implementing this policy consistently

- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (Appendix 2), and ensuring that pupils follow the school's terms on acceptable use (Appendix 1)

- Working with the SBM, DSL, Curriculum Lead, RM, Soft Egg to ensure that any online safety incidents are logged (see Appendix 4) and dealt with appropriately in line with this policy

- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy (see Responding to an Online Safety Concern flowchart)

3.6 Parents and carers

Parents and carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy

- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (Appendix 1)

Parents and carers can seek further guidance on keeping children safe online by using the information provided on the school website (see safety on the web section)

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 2). Please note that this is subject to any amendments from GDPR 25th May 2018

Visitors and members of the community are expected to demonstrate and role model appropriate use of online technologies

3.8 It is the responsibility of pupils (at a level that is appropriate to their individual age, ability and vulnerabilities) to:

- Engage in age appropriate online safety education opportunities.

- Contribute to the development of online safety policies.

- Read and adhere to the school Acceptable Use Policy (AUP).

- Respect the feelings and rights of others both on and offline.

- Take responsibility for keeping themselves and others safe online.

- Seek help from a trusted adult, if there is a concern online, and support others that may be experiencing online safety issues.

4. ICT in the curriculum

- Ashford Park uses a wide range of technology. This includes access to:
  - Computers, laptops, LearnPads and other digital devices
  - Internet which may include search engines and educational websites
  - School learning platform/intranet
  - Games consoles and other games based technologies
  - Digital cameras, web cams and video cameras
- All school owned devices will be used in accordance with the school's Acceptable Use policy (AUP) and with appropriate safety and security measures in place.
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
- The school will use age appropriate search tools, following an informed risk assessment, to identify which tool best suits the needs of our community.
- The school will ensure that the use of internet-derived materials, by staff and pupils, complies with copyright law and acknowledge the source of information.
- Supervision of pupils will be appropriate to their age and ability.

Pupils will be taught about online safety as part of the curriculum.

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact
- How to report a range of concerns

The safe use of social media and the internet will also be covered in other subjects where relevant.

The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

4.1 Pupils' Personal Use of Social Media

- Safe and appropriate use of social media will be taught to pupils as part of an embedded and progressive education approach, via age appropriate sites and resources.
- The school is aware that many popular social media sites state that they are not for children under the age of 13, therefore the school will not create accounts specifically for children under this age.
- Any concerns regarding pupils' use of social media, both at home and at school, will be dealt with in accordance with existing school policies including anti-bullying and behaviour. Concerns will also be raised with parents/carers as appropriate, particularly when concerning underage use of social media sites or tools.
- Pupils will be advised:
  - To consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location. Examples would include real/full name, address, mobile or landline phone numbers, school attended, other social media contact details, email addresses, full names of friends/family, specific interests and clubs.
  - To only approve and invite known friends on social media sites and to deny access to others by making profiles private/protected.
  - Not to meet any online friends without a parent/carer or other responsible adult's permission and only when a trusted adult is present.
  - To use safe passwords.
  - To use social media sites which are appropriate for their age and abilities.
  - How to block and report unwanted communications and report concerns both within school and externally.

4.2 Support for vulnerable pupils

- Ashford Park is aware that some pupils are considered to be more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with

Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.

- Ashford Park will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable pupils.
- Ashford Park will seek input from specialist staff as appropriate, including the SENCO, Child in Care Lead.

5. Educating parents and carers about online safety

The school will raise parents' and carers awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents/carers.

Online safety will also be covered during parents' evenings as part of the taught curriculum.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

6. Cyber-bullying or Online bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour for learning policy.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their classes, and the issue will be addressed in assemblies and arranged learning opportunities e.g. Just Joshing (anti-bullying workshop) and Kidscape (anti-bullying policy).

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school provides links to websites that provide information regarding online safety. This can be found on the school website.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school anti-bullying policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so (as set out in the Responding to an Online Safety concern flowchart).

7. Acceptable use of the internet in school

All pupils, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (Appendices 1 and 2). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in Appendices 1 and 2.

Staff:

- The use of personal email addresses by staff for any official school business is not permitted.
  - o All members of staff are provided with a specific school email address, to use for all official communication.
- Members of staff are encouraged to have an appropriate work life balance when responding to email, especially if communication is taking place between staff and pupils and parents/carers.

Educational use of Video conferencing and/or Webcams

- Ashford Park recognise that video conferencing use of webcams can be a challenging activity but brings a wide range of learning benefits.
  - o All video conferencing and webcam equipment will be switched off when not in use and will not be set to auto-answer.
  - o Video conferencing equipment connected to the educational broadband network will use the national E.164 numbering system and display their H.323 ID name; external IP addresses will not be made available to other sites.
  - o Video conferencing contact details will not be posted publically.
  - o School video conferencing equipment will not be taken off school premises without prior permission from the DSL.
  - o Staff will ensure that external video conferencing opportunities and/or tools are suitably risk assessed and will ensure that accounts and systems used to access these events are safe and secure.
  - o Video conferencing equipment and webcams will be kept securely and, if necessary, locked away or disabled when not in use.

8. Pupils using mobile devices in school

Pupils in Year 6 may bring mobile devices into school, to be able to communicate with parents/carers when walking home, but they must be handed into the office and they are not permitted to use them throughout the school day.

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see Appendix 1).

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

If a pupil needs to contact his/her parents or carers they will be allowed to use a school phone.

9. Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 2.

Staff must ensure that their work device is secure, encrypted and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the SBM, DSL, Curriculum Lead, RM or Soft Egg.

Work devices must be used solely for work activities.

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in the behaviour for learning policy and the Responding to an Online Safety Concern flowchart. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures, following the Responding to an Online Safety Concern flowchart. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

All new staff members will receive training, as part of their induction, on safeguarding and child protection including prevent.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

The DSL will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

It is the expectation of governors to read part 1 and pat 2 of the 'Keeping Children Safe in Education' document (September 2016).

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

12. Monitoring arrangements

The SBM, DSL, Curriculum Lead, RM and Soft Egg log behaviour and safeguarding issues related to online safety. An incident report log can be found in Appendix 4.

This policy will be reviewed annually by the computing lead. At every review, the policy will be shared with the governing board and the school community.

Security and Management of Information Systems

- The school takes appropriate steps to ensure the security of our information systems, including;
  - o Virus protection being updated regularly.
  - o Encryption for personal data sent over the Internet or taken off site (such as via portable media storage) or access via appropriate secure remote access systems.
  - o Not using portable media without specific permission; portable media will be checked by an anti-virus /malware scan before use.
  - o Not downloading unapproved software to work devices or opening unfamiliar email attachments.
  - o Regularly checking files held on the school's network,
  - o The appropriate use of user logins and passwords to access the school network.
  - o All users are expected to log off or lock their screens/devices if systems are unattended.

13. Links with other policies

This online safety policy is linked to our:

- Anti-Bullying policy
- Child protection and safeguarding policy
- Behaviour for learning policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure

Appendix 1: Acceptable use agreement (pupils and parents/carers)

Acceptable use of the school's ICT systems and internet: agreement for pupils and parents/carers

Name of pupil:

When using the school's ICT systems and accessing the internet in school, I will not:

- Use them for a non-educational purpose
- Use them without a teacher being present, or without a teacher's permission
- Access any inappropriate websites
- Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity)
- Use chat rooms
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Share my password with others or log in to the school's network using someone else's details
- Give my personal information (including my name, address or telephone number) to anyone without the permission of my teacher or parent/carer
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

If I bring a personal mobile phone or other personal electronic device into school:

- I will not use it during the school day, in clubs or other activities organised by the school, without a teacher's permission
- I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online
- I will hand it in to be securely stored in the school office.

I agree that the school will monitor the websites I visit.

I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others.

I will always use the school's ICT systems and internet responsibly as described above, for example.

Signed (pupil):	**Date:**

Parent/carer agreement: I agree that my child can use the school's ICT systems and

internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 2: Acceptable use agreement (staff, governors, volunteers and visitors)

.

Acceptable use of the school's ICT systems and the internet: agreement for staff, governors, volunteers and visitors
Name of staff member/governor/volunteer/visitor:
When using the school's ICT systems and accessing the internet in school, or outside school on a work device, I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature • Use them in any way which could harm the school's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software • Share my password with others or log in to the school's network using someone else's details • To not take part in any activity that would be a detriment to your professional reputation, see part 2 of the teacher standards
I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the school will monitor the websites I visit. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) and SBM, Curriculum Lead, RM or Soft Egg know if a pupil informs me they have found any material which might upset, distress or harm

them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 3: online safety training needs – self-audit for staff

Online safety training needs audit	
Name of staff member/volunteer:	**Date:**
Do you know the name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents/carers?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	

Are there any areas of online safety in which you would like training/further training? Please record them here.	

Appendix 4: online safety incident report log

Online safety incident report log				
Date	Where the incident took place	Description of the incident	Action taken	Name and signature of staff member recording the incident